

Kathleen Fisher
Program Manager, Information Innovation Office

High Assurance Systems

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 07 NOV 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE High Assurance Systems				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, 3701 North Fairfax Drive, Arlington, VA, 22203-1714				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 8	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Physical systems vulnerable to cyber attacks



Falsified
speedometer
reading:
140 mph in [P]ark!

K. Koscher, et al. "Experimental Security Analysis of a Modern Automobile," in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.



Many remote attack vectors

Long-range wireless



Indirect physical
Entertainment



Short-range wireless



Mechanic

Image sources: www.autoblog.com,
www.journalofamrangler.com, www.1800pocketpc.com,
en.wikipedia.org/wiki/Compact_Disc www.thedigitalbus.com,
coolmaterial.com, www.laptopsarena.com, www.elec-intro.com,
mybluetoothearbuds.blogspot.com, www.diytrade.com



Pervasive vulnerability

SCADA Systems



Computer Peripherals



Vehicles



Medical Devices



Communication Devices



Sources:
en.wikipedia.org/wiki/File:Gas_centrifuge_cascade.jpg,
gis-rci.montpellier.cemagref.fr, cybersecure.com,
www.ourestatesale.com, www.eweek.com,
pastorron7.wordpress.com, landsat.gsfc.nasa.gov,
www.tech2date.com, www.militaryaerospace.com,
www.naval-technology.com, www.chinacartimes.com



We need a fundamentally different approach

- State of the art:
 - Anti-virus scanning, intrusion detection systems, patching infrastructure
- This approach *cannot* solve the problem.
 - Focused on known vulnerabilities; can miss zero-day exploits
 - Can introduce new vulnerabilities and privilege escalation opportunities

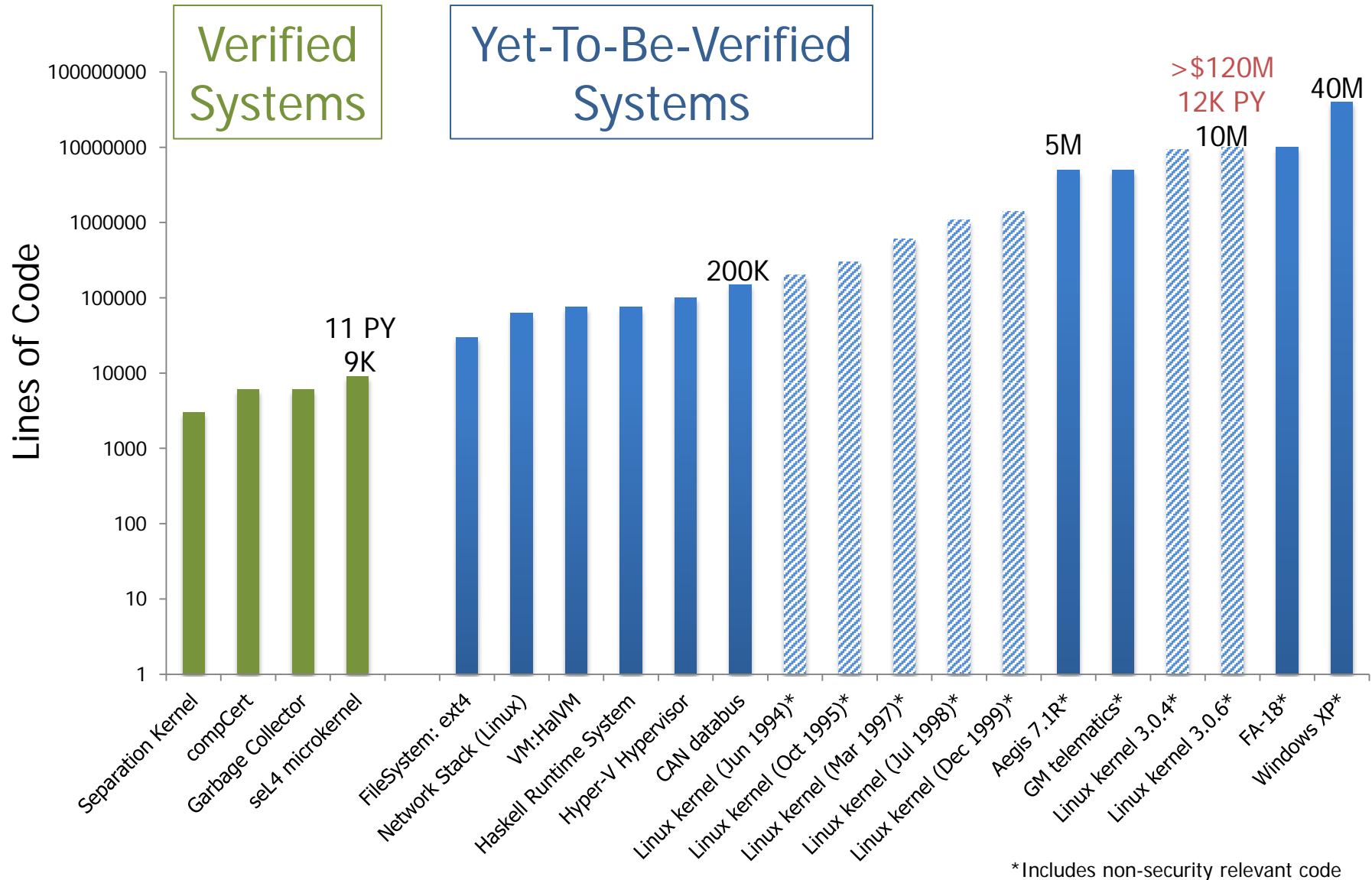
October 2010 Vulnerability Watchlist

Vulnerability Title	Fix Avail?	Date Added
XXXXXXXXXX XXXXXXXXXXXX Local Privilege Escalation Vulnerability	No	8/25/2010
XXXXXXXXXX XXXXXXXXXXXX Denial of Service Vulnerability	Yes	8/24/2010
XXXXXXXXXX XXXXXXXXXXXX Buffer Overflow Vulnerability	No	8/20/2010
XXXXXXXXXX XXXXXXXXXXXX Sanitization Bypass Weakness	No	8/18/2010
XXXXXXXXXX XXXXXXXXXXXX Security Bypass Vulnerability	No	8/17/2010
XXXXXXXXXX XXXXXXXXXXXX Multiple Security Vulnerabilities	Yes	8/16/2010
XXXXXXXXXX XXXXXXXXXXXX Remote Code Execution Vulnerability	No	8/16/2010
XXXXXXXXXX XXXXXXXXXXXX Use-After-Free Memory Corruption Vulnerability	No	8/12/2010
XXXXXXXXXX XXXXXXXXXXXX Remote Code Execution Vulnerability	No	8/10/2010
XXXXXXXXXX XXXXXXXXXXXX Multiple Buffer Overflow Vulnerabilities	No	8/10/2010
XXXXXXXXXX XXXXXXXXXXXX Stack Buffer Overflow Vulnerability	Yes	8/09/2010
XXXXXXXXXX XXXXXXXXXXXX Security-Bypass Vulnerability	No	8/06/2010
XXXXXXXXXX XXXXXXXXXXXX Multiple Security Vulnerabilities	No	8/05/2010
XXXXXXXXXX XXXXXXXXXXXX Buffer Overflow Vulnerability	No	7/29/2010
XXXXXXXXXX XXXXXXXXXXXX Remote Privilege Escalation Vulnerability	No	7/28/2010
XXXXXXXXXX XXXXXXXXXXXX Cross Site Request Forgery Vulnerability	No	7/26/2010
XXXXXXXXXX XXXXXXXXXXXX Multiple Denial Of Service Vulnerabilities	No	7/22/2010

1/3 of the vulnerabilities
are in security software!



Critical Components within Reach of Formal Methods

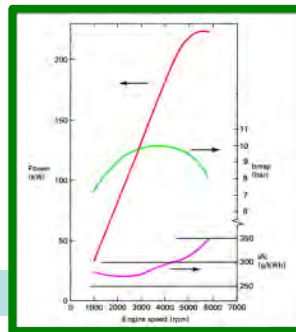




High-Assurance Component Factory



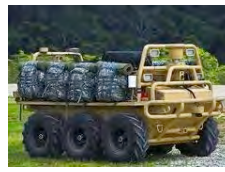
Cyber



Physical

Key Challenges

- Reusable components
- Composition
- Increasing automation
- Scaling
- Concurrency
- Cyber-physical integration



Sources: en.wikipedia.org/wiki/File:Gas_centrifuge_cascade.jpg, gis-rci.montpellier.cemagref.fr, cybersecure.com, www.ourestatesale.com, www.tech2date.com, www.eweek.com, dronewarsuk.wordpress.com

High Assurance: Correctness, Safety, Security



Feedback welcome!

- Promising research directions?
- Additional challenges?
- Other things you think I should know?

Contact Information: Kathleen.Fisher@darpa.mil